View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repositorio Institucional UniLibre

DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMATICA PARA LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTÁ.

ANDRES PALACIOS ORTEGA
CÓDIGO: 066092028

UNIVERSIDAD LIBRE DE COLOMBIA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2015

DISEÑO DE UN MODELO DE POLÍTICAS DE SEGURIDAD INFORMATICA PARA LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTÁ.

PROYECTO DE GRADO PRESENTADO COMO REQUISITO PARA OBTENER EL TITULO DE INGENIERO DE SISTEMAS

ANDRES PALACIOS ORTEGA
CÓDIGO: 066092028

ING. FABIÁN BLANCO GARRIDO
Director de Proyecto

UNIVERSIDAD LIBRE DE COLOMBIA
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2015

CALIFICACION

_____

_____

_____

_____
Ing. Juan Fernando Velásquez C
Director de Programa

_____
Ing. Fabián Blanco G
Presidente Jurado

Mauricio Alonso Moncada
Jurado

Eduardo Triana M
Jurado

Bogotá D.C, 03 De Septiembre de 2015.

DEDICATORIA

Inicialmente deseo dedicarle este trabajo especial a todas las personas que siempre creyeron en mi capacidad, capacidad que tenemos todos, es grato saber la fuerza y determinación que poseemos cuando queremos alcanzar algo.

A mis padres, mama (María Ilma Ortega Torres), Papa (Isidro Palacios Sarmiento), no hay un día en el que no le agradezca a dios el haberme colocado entre ustedes, la fortuna más grande es tenerlos conmigo y el tesoro más valioso son todos y cada uno de los valores que me inculcaron.

AGRADECIMIENTOS

Le damos gracias a Dios por permitirnos concluir esta etapa, por darnos la paciencia y la voluntad para terminar nuestra carrera y aprender de nuestros errores como seres humanos.

A nuestras familias por su apoyo incondicional, por ser nuestros mejores ejemplos a seguir y por sus consejos.

TABLA DE CONTENIDO

Contenido **PAGINA**

LISTADO DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

Este proyecto define políticas de seguridad en la Súper Intendencia de Industria y Comercio (SIC) de Bogotá. En primera instancia se realizó un diagnóstico de las diferentes vulnerabilidades que presenta la entidad a nivel de seguridad informática. Esto significa que el proyecto ha sido elaborado para ofrecer un modelo de implementación, operación seguimiento, revisión, mantenimiento y mejoramiento continuo de las políticas de seguridad informática.

En Conclusión el proyecto se fundamenta con diferentes lineamientos de la seguridad informática establecida por la norma ISO 27001 que buscan la confidencialidad, integridad y disponibilidad de la información de la SIC.

Palabras Clave: Seguridad, Información, confidencialidad, integridad, disponibilidad

ABSTRACT

This project defines security policies in the Super Administration of Industry and Commerce (SIC) of Bogota. A diagnosis of the different vulnerabilities that introduces the entity-level security was held at first instance. This means that the project has been prepared to provide a model implementation, operation monitoring, review, maintenance and continuous improvement of information security policies.

In conclusion, the project is based with different computer security guidelines established by the ISO 27001 seeking confidentiality, integrity and availability of information to the SIC.

Keywords: safety, information, confidentiality, integrity, availability

INTRODUCCIÓN

La presente investigación se refiere al tema de un diseño de políticas de seguridad informática para la SIC, que se puede definir como la interacción entre los usuarios y los gerentes, que establecen el canal formal de actuación del personal en relación con los recursos y servicios informáticos, importantes de la organización.

La característica principal de las políticas de seguridad es asegurar el buen funcionamiento y facilitar los procesos para los usuarios tanto internos como externos de la Superintendencia de Industria y Comercio de Bogotá, mejorando sus módulos a nivel de seguridad, ya que ellos contienen información de gran impacto.

Para analizar esta problemática es necesario realizar un diagnóstico para identificar las falencias que presenta el sistema de seguridad informática. En consecuencia dichas falencias se presentan por la ausencia de protocolos de seguridad, que conllevan a que los sistemas de información sean más vulnerables a fugas de información.

1. MARCO OPERACIONAL DE DESARROLLO

1.1 Identificación del proyecto.

“Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá.”

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 DESCRIPCIÓN DEL PROBLEMA

A nivel mundial los mayores incidentes en la seguridad informática se manifiestan por diferentes factores que incrementan los riesgos en la perdida de la información. De acuerdo a la investigación establecida por el Doctor Andrés Ricardo Almanza se identifica cuatro incidentes principales, el primer incidente se relaciona con la instalación de software no autorizado con el (55,56%), En segundo lugar se identifica los Virus/Caballos de Troya (46,3%), el tercer incidente acceso no autorizados a la web. En consecuencia la fuga de información sigue en la escala de lo identificado (19,14%), lo que muestra el panorama actual de los peligros existentes. A nivel Nacional la tendencia en incidentes se mantiene en Colombia (SIC, 2015).

A nivel distrital se identifican algunas problemáticas con los Sistemas de Gestión de Seguridad Informática (SGSI) como es el caso particular de la Superintendencia de Industria y Comercio (SIC), la primera falencia identificada se encuentra referida a la infraestructura puesto que sus instalaciones son viejas y puede ocasionar un desastre, la segunda falencia se encuentra referida a los ingresos o a centros de cómputo no autorizados, la tercera se refiere a la falta de actualización de software en todos los equipos de la entidad. La carencia de políticas de seguridad y el manejo inadecuado de los usuarios en una entidad pública que fortalece los procesos de desarrollo empresarial en Colombia, puede representar afectaciones al sector empresarial del País.

1.2.2 FORMULACION DEL PROBLEMA

¿Cómo Diseñar un modelo de políticas de seguridad para proteger la información en la superintendencia de industria y comercio?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Diseñar un Modelo de políticas de seguridad de la información para la protección de los datos en la Superintendencia de Industria y Comercio de Bogotá.

1.3.2 OBJETIVOS ESPECÍFICOS

- Hacer un diagnóstico de análisis de riesgos para proporcionar un panorama general de las vulnerabilidades en las diferentes áreas presentes en la SIC.
- Analizar los resultados obtenidos para identificar factores y áreas vulnerables.
- Construir una matriz de vulnerabilidades para diseñar el modelo de políticas de la SIC.

1.4 JUSTIFICACIÓN

En la actualidad la Superintendencia de Industria y Comercio (SIC), presenta grandes falencias de seguridad de la información en las diferentes áreas de la entidad, por tanto es preciso revisar las diferentes vulnerabilidades que se presenta en la protección de los datos y los lineamientos de la entidad para la seguridad de la información.

En razón a lo anterior es preciso diseñar un modelo de políticas de seguridad informática para solucionar los diferentes incidentes que se presentan en la SIC y el desarrollo de mecanismos que ayuden a mitigar impactos de la seguridad de la información, puesto que éstos pueden ser puntos críticos para el desarrollo de las actividades de la SIC.

Con el fin de cumplir con el modelo de políticas, se requiere contar con un profesional ingeniero de sistemas, que apoye proyectos de solución informática y desarrolle servicios de monitoreo y un plan de auditorías en proyectos de seguridad informática. Si bien el desarrollo de la presente investigación complementa los diferentes procesos que adelanta la SIC en la implementación de la norma ISO 27001, por lo cual se requiere un control y seguimiento especial en dicho proceso, que debe ser de carácter permanente.

1.5 ALCANCE

Esta investigación solo tomara en cuenta el estudio y análisis de la seguridad de la información en la SIC referente al problema de delito informático, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega la auditoria informática ante este tipo de amenaza.

1.6 MARCO INVESTIGATIVO

1.6.1 TIPO DE INVESTIGACION

Por las características del proyecto y naturaleza lógica del entregable, el marco referencial lo constituye la investigación tecnológica aplicada.

1.6.2 METODOLOGIA

El tipo de investigación que se ha elegido para el desarrollo del proyecto es el cuantitativo, debido a que podemos obtener el conocimiento y elegir un modelo adecuado que nos permita conocer la realidad del objeto de estudio y poder analizar los datos recolectados por medio de los conceptos y las variables que se manejen.

La metodología que se va a llevar a cabo está basada en las normas ISO/IEC 27001, de acuerdo a las necesidades de la Superintendencia de Industria y Comercio de Bogotá. La metodología irá de la mano con los objetivos planteados en el proyecto para su consecución.

Primero, se realizará un levantamiento de información de las prácticas de seguridad y del estado de la misma en la organización. La salida de este proceso, entregará el insumo base para poder realizar el análisis de las políticas existentes y así determinar cuales se mantienen, se modifican o deben elaborar.

Posteriormente, con el trabajo realizado se establecerán los requisitos para la elaboración de las políticas adecuadas que garanticen la seguridad de la información.

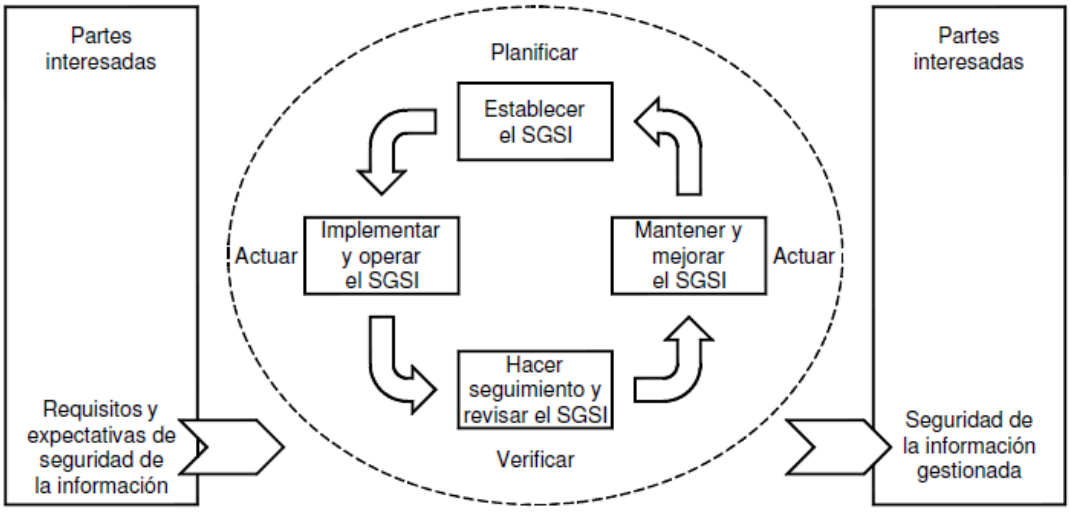

Figura 1. Modelo PHVA aplicado a los procesos de SGSI

Finalmente se dará a conocer a los funcionarios y directivos de la Superintendencia de industria y comercio de Bogotá, el plan de buenas prácticas en el uso de los sistemas de información que están dispuestos para el desarrollo de sus labores, para minimizar el riesgo de pérdida, daño o alteración en la información, o para saber cómo actuar en el momento de una violación de seguridad, ya sea de una fuente interna o externa.

2. FUNDAMENTACION TEORICA FUNCIONAL

2.1 MARCO HISTÓRICO

A continuación se detallan para efectos de interpretación y documentación del trabajo, las características inherentes al núcleo formal de desarrollo.

2.1.1 SEGURIDAD INFORMATICA

Este capítulo trata sobre la historia de los estándares de seguridad informática. La seguridad informática ha sido un aspecto fundamental de la computación digital durante décadas, puesto que su inicio y la financiación anticipada del Departamento de Defensa (DoD), pero con la evolución de la industria y la academia se convierten aún más prevalente en las últimas dos décadas. Si bien el Departamento de Defensa sigue siendo una fuerza en tanto la computación en red y la seguridad informática, su lugar relativo ha disminuido hasta el punto porque la industria de la computación grande y vibrante ha sido el epicentro de muchos desarrollos de tecnología informática y el comercio de software de seguridad se ha convertido en un sector fundamental de la seguridad de TI. La posición preeminente de los Estados Unidos en las normas de seguridad informática, ha disminuido la importancia de la investigación en todo el mundo, y las normas internacionales se han vuelto más crítico en un entorno cada vez más global y económico. Por consiguiente las Normas son creadas por las demandas del mercado y las interacciones empresariales. (Yost, 2007)

A mediados del siglo XIX se han desarrollado sistemas de clasificación más complejos para que los gobiernos puedan gestionar su información de acuerdo con el grado de sensibilidad

El final del siglo XX y principios del siglo XXI vio a los rápidos avances en telecomunicaciones, la informática de hardware y software, y el cifrado de datos. La disponibilidad de equipo de -cómputo más pequeño, más potentes y menos costosos hizo procesamiento electrónico de datos al alcance de las pequeñas empresas y los usuarios domésticos. Estos ordenadores se convirtieron rápidamente en interconectados a través de una red genéricamente se llama Internet.

El rápido crecimiento y el uso generalizado de procesamiento electrónico de datos y comercio electrónico realizado a través de Internet, junto con numerosos casos de terrorismo internacional, alimentaron la necesidad de mejorar los métodos de protección de los equipos y la información que almacenan, procesan y transmiten. Las disciplinas académicas de la seguridad informática y seguridad de la información surgió junto con numerosas organizaciones profesionales - que comparten los objetivos comunes de garantizar la seguridad y fiabilidad de los sistemas de información. (Docsetools, 2015).

2.2 MARCO TEÓRICO

ANÁLISIS DE RIESGOS

La política de seguridad analiza las diferentes directrices de una organización, formando parte de la política general, por tanto debe ser cercana a la alta dirección de la compañía. Si bien el objetivo general en la redacción de dicha política debe concienciar a los empleados y contratistas, en consecuencia en preciso involucrar un sistema de información, puesto que la política de seguridad informática se debe estructurar con cinco puntos importantes que permite identificar, relacionar, proporcionar, detectar y definir todas aquellas falencias de seguridad informática para realizar una evaluación del impacto que pueden darse en la entidad. Dentro de las herramientas más destacadas para el análisis de riesgos tenemos:

- MAGERIT: Es una metodología de análisis y gestión de riesgos de los sistemas de información.
- PILAR: Es un procedimiento informatico-logico para el análisis y gestión de riegos, que sigue la metodología MAGERIT. (Aguilera, 2010).

El análisis y gestión de riesgos introduce un enfoque riguroso para la identificación de factores que tiene la organización, esto implicaría una violación de seguridad de la empresa. Bajo el marco en la identificación de vulnerabilidades y amenazas

es importante establecer medidas que permitan reducir perdidas de la información. (Heredero, y otros, 2006).

SEGURIDAD INFORMATICA

Se define como la “Protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo”.

Para poder detener las amenazas se necesita poner un alto, pero ninguna protección es infalible, es necesario multiplicar las barreras, así un pirata que intenta ingresar será bloqueado por otra barrera.

Para elegir un nivel de seguridad adaptado implica consecuencias ligadas a restricciones para los usuarios, la carga financiera por la adquisición de programas de protección, tiempo para implementar estas soluciones, y mejoras en las instalaciones. (Royer, 2004).

La inseguridad en sistemas informáticos se debe a un gran número de amenazas que circulan en el internet. Por esta razón los niveles de seguridad para la una organización deben ser altísimos, ya que podrían tener fugas de información sensible para ellos, no es solo con una actualización continua de antivirus ya que con esto aún nuestro sistema es inseguro, se deben implementar otros tipos de software que impidan el acceso no autorizado para terceras personas que no pertenecen a la organización.

Confidencialidad hablamos de confidencialidad cuando no referimos a la característica que asegura que los usuarios sean (personas, procesos, etc.), no tengan acceso a los datos a menos que estén autorizados para ello.

Disponibilidad garantiza que los recursos de sistema y la información estén disponibles solo para usuarios autorizados en el momento en que los soliciten.

Integridad nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos también autorizados.

(Cerra, 2010).

Nunca se van a conocer todos los tipos de ataques posibles. Es imposible lograr una seguridad optima no hay nadie que pueda abarcar todo lo hecho y todo lo que se puede estar haciendo ahora, así que un profesional debe conformarse por conocer el gran número de ataques posibles y estar muy bien informado con lo que se está haciendo, de esta manera es posible crear o diseñar programas para evitar estos ataques. Los ataques más importantes son los ataques para obtener información, ataques de acceso no autorizado, ataques con revelación de información y ataques de degeneración de servicios y para el atacante puede hacer combinaciones de estos ataques. (Diaz, Mur, San Cristobal, Castro, & Peire, 2012).

Un sistema de gestión de seguridad necesita medidas de seguridad técnicas de procedimiento, físicas, lógicas, de persona y de gestión. Esto hace que se englobe una serie de actividades que consisten en la valoración de las amenazas y saber en qué estado se encuentran por consiguiente el SGSI es parte del sistema global basado en los riesgos del negocio y saber que establece, implementa, opera, monitorea, revisa, mantiene, y mejora la seguridad de la información. Dicho sistema debe incluir políticas y actividades para las buenas prácticas con los empleados y contratistas de la entidad para preservar la seguridad de la información en la organización. (Bertolin, 2008)

2.3 Norma Técnica ISO/IEC 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.
El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. (Academic, 2015).

La norma ISO/IEC 27001 ha sido reconocida por 1870 organizaciones en 57 países donde es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y es aplicable a todo tipo de organizaciones sin importar su tamaño o actividad. (Estrada, 2011)

Ver anexo de la norma ISO 27001.

2.4 Fundamentos de Seguridad Informática

Un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de información de una organización. Los servicios están

dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Clasificación

Una clasificación muy utilizada de los servicios de seguridad es la siguiente:

- Confidencialidad
- Autenticación
- Integridad
- No repudio
- Control de acceso (Universidad Autonoma de Mexico, 2014)

2.5 MARCO CONCEPTUAL

El conjunto de entidades cuya lógica e integridad de significación, sustentan la construcción del entregable definido, se enuncian para sus efectos a continuación:

ADWARE: Es un programa de internet que cuando se ejecuta, muestra publicidad de internet y la descarga. El principal síntoma de infección de adware es la aparición de ventanas emergentes en nuestra computadora.

CONFIDENCIALIDAD: Hablamos de confidencialidad cuando no referimos a la característica que asegura que los usuarios sean (personas, procesos, etc.), no tengan acceso a los datos a menos que estén autorizados para ello.

DISPONIBILIDAD: Garantiza que los recursos de sistema y la información estén disponibles solo para usuarios autorizados en el momento en que los soliciten.

INTEGRIDAD: Nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos también autorizados.

SPYWARE: Es un programa espía que se instala sin autorización del cliente, y su objetivo es conocer los hábitos informáticos del usuario de la computadora. Esta

información es enviada vía e-mail por empresas publicitarias. Se transmiten a través de adjuntos de correo electrónicos y programas descargados de sitios no confiables. (Cerra, 2010).

ISO: International Standards Organization. Una de las organizaciones de normalización más importantes .El gobierno de cada país está representado individualmente. (Diaz, Mur, San Cristobal, Castro, & Peire, 2012)

2.6 MARCO LEGAL

LEY ESTATUTARIA 1581 DE 2012.

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan

una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
4. Crea una especial protección a los datos de menores de edad.
5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
8. Crea el Registro Nacional de Bases de Datos.
9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos. (UNAD, 2015)

LEY 1273 DE 2009 (Enero 05)

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del

territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II
De los atentados informáticos y otras infracciones
Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (MINITIC, s.f.)

PROYECTO DE LEY 241 DE 2011 SENADO

Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.

El Congreso de Colombia

DECRETA:

CAPÍTULO I

Criterios de Responsabilidad

Artículo 1°. Prestadores de servicios de internet. A los efectos de esta ley se entenderán por tales las personas que presten uno o varios de los siguientes servicios:

a) Transmitir, enrutar o suministrar conexiones para materiales sin hacer modificaciones en su contenido;

b) Almacenar datos temporalmente mediante un proceso automático (caching);

c) Almacenar a petición de un usuario del material que se aloja en un sistema o red controlado u operado por o para el prestador de servicios; y

d) Referir o vincular a los usuarios a un sitio en línea mediante la utilización de herramientas de búsqueda de información, incluyendo hipervínculos y directorios.

Ver anexo de la ley proyecto de ley 241 de 2011 senado.

3. CONSTRUCCION DE LA SOLUCION INGENIERIL

La Superintendencia de industria y comercio de Bogotá (SIC) en la entidad del estado orientado a fortalecer los procesos de desarrollo empresarial y los niveles de satisfacción del consumidor colombiano. Para entender las diferentes funciones en la sic es preciso conocer la misión y la visión:

Misión

La SIC salvaguarda los derechos de los consumidores, protege la libre y sana competencia, actúa como autoridad nacional de la propiedad industrial y defiende los derechos fundamentales relacionados con la correcta administración de datos personales.

De esta manera, la SIC es parte fundamental en la estrategia estatal en favor de la competitividad y la formalización de la economía, lo cual incluye la vigilancia a las cámaras de comercio y la metrología legal en Colombia.

Visión

Seremos reconocidos como una Entidad líder en el control y apoyo a la actividad empresarial y en la defensa de los derechos del consumidor colombiano y de la protección de datos personales.

Para el efecto, se consolidará una estructura administrativa soportada en un talento humano que se distinguirá por su profesionalismo y compromiso y con una clara orientación de servicio al país y en un sistema integrado de gestión, apoyado en procesos automatizados que atenderán los requerimientos de los usuarios institucionales. (SIC, 2015).

3.1 Organización Interna

La gerencia apoya activamente la implementación de estas políticas de seguridad con el estudio realizado en este proyecto. Por otra parte, todos los funcionarios tienen conocimiento de la implementación de este proyecto y están comprometido con el desarrollo del mismo, siendo participes activos, con claras responsabilidades definidas en su puesta en marcha.

3.2 Entidades Externas

Se debe tener una normatividad clara cuando entidades externas trabajan para la Superintendencia de Industria y Comercio de Bogotá y cuando se requiere compartir información o acceder a los recursos de red y/o tecnológicos.

3.3 GESTIÓN DE ACTIVOS

Responsabilidad por los activos

Se cuenta con mil doscientos (1200) equipos de cómputo, servidores los cuales cincuenta (50) están en físico y ciento cincuenta (150) son virtuales, novecientos (900) teléfonos voz IP físicos y un doscientos (200) teléfonos Softphone, dentro de su inventario.

Por parte de los computadores, se observó que dichas máquinas tienen diferentes características y algunas máquinas no tienen un buen rendimiento de acuerdo a las tareas que desarrolla el funcionario.

Hay máquinas desde 4 Gb hasta 8 Gb en memoria RAM, discos duros desde 500 Gb hasta 1 Tb, procesadores desde Core i3 Duo hasta Core i5 de 3era generación; en resumen la brecha tecnológica entre estos dispositivos no es tan amplia, pero puede ser significativa en el corto plazo. Se encuentran tres tipos de sistemas operativos: Windows 7, Windows 8 y OS X Lion. Se maneja la versión 2010 y 2013 de Office (Hogar y Pequeña Empresa) para los equipos bajo la plataforma Windows y Office 2011 (Hogar y Empresas) para el equipo MacBook.

Los equipos con mayor tiempo de uso, ya presentan bloqueos funcionales que pueden durar minutos, problemas con algunas unidades de DVD y discos duros (ya han sido reemplazados dos discos) demoras en la conexión de red e inconvenientes en el apagado de algunos monitores. Esto ha generado retrasos y fallos a la hora de desempeñar alguna actividad propia de la Súper Intendencia.

El área de sistemas de esta organización maneja una hoja de vida de los equipos existentes dentro de la empresa, donde se tiene documentos como las cotizaciones que se tuvieron en cuenta para adquirir el equipo, copia de la factura de compra, y diferentes documentos de reparaciones y garantías. Este requisito no lo cumplen todos los equipos en existencia de la empresa, por lo que a veces es difícil determinar la historia de los equipos cuando presentan fallas.

Casi todos los equipos están rotulados con un número de identificación, que está relacionado en el inventario general de la Súper Intendencia. Esto es un riesgo para la seguridad de los equipos ya que al no tener estas etiquetas en su totalidad no se tiene un control sobre estos los activos

Posee documentación sobre el uso que se le debe dar a los equipos, es por ello que los usuarios al momento de darle un uso no adecuado, no se les podría establecer un llamado de atención por este mal uso.

3.4 POLÍTICAS DE SEGURIDAD INFORMATICA EN LA SUPERINTENDECIA DE INDISTRIA Y COMERCIO DE BOGOTA.

Las políticas de seguridad Informática realizadas, después del análisis previo de riesgos, amenazas y vulnerabilidades en la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTÁ se describen a continuación:

3.4.1 Política General En Seguridad de la Información

El área de sistemas es el ente encargado de velar por la seguridad informática,
Estas políticas van dirigidas a todo el personal, contratistas y visitantes de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA. Se espera que permitan definir los comportamientos esperados, para reducir la manifestación de riesgos que afecten la seguridad de la información de la empresa.

Los Gerentes y coordinadores de cada área son responsables de velar por el cumplimiento de estas políticas. En caso de no entendimiento de las mismas, tramitar consulta al área de seguridad de la información de la empresa.

3.4.2 DIRECTRICES

Dando cumplimiento a las acciones tomadas por las directivas de la compañía para dar respuesta en su mejora continua y compromiso en la prestación de sus servicios, garantizando la seguridad de la información y teniendo en cuenta la responsabilidad adquirida ante nuestros clientes, accionistas, empleados,

proveedores y estado, el Comité de Seguridad de la Información de la empresa ha definido y decidido aplicar la siguiente política de seguridad:

LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA, propenderá por garantizar la Confidencialidad, Integridad y Disponibilidad de los activos de información de la compañía, sus clientes y proveedores; con el desarrollo y operación de servicios en Seguridad de la Información.

3.4.3 Política de Respaldo y Recuperación de la Información.

La información es un activo de la SUPER INTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA y por lo tanto es responsabilidad de todos los usuarios darle un buen uso y protegerla.

La información almacenada en los servidores, equipos de comunicaciones y en general cualquier sistema de información de la compañía, debe respaldarse para evitar perdida de información o para recuperar el estado anterior en caso de fallas. Se debe definir el sistema, el contenido a respaldar, el tipo de respaldo, el medio, la frecuencia y la ubicación. Esta información la define el líder de proceso/proyecto, con el apoyo de la coordinación de plataforma.

3.4.4 DIRECTRICES.

- **Los backups de los sistemas deben retenerse por un tiempo límite definido.**

  Explicación: Es importante definir un tiempo límite de (6) seis meses de retención para cada sistema, que se ajuste a las necesidades y criticidad del mismo. El tiempo límite es definido por el líder de proceso/proyecto, con

el apoyo de la coordinación de plataforma. Después de cumplido el tiempo de retención, los backups pueden eliminarse.

- **La destrucción o reutilización de los medios de almacenamiento debe realizarse de manera segura.**

Explicación: Se deben establecer procedimientos formales para la destrucción o reutilización segura de los medios que contengan información confidencial. Los procedimientos de eliminación deben ser proporcionales a la sensibilidad de la información, definidos por el Área Seguridad de la Información.

- **El acceso a las instalaciones y medios de almacenamiento de los backups debe ser restringido.**

Explicación: Las instalaciones donde se almacenan los backups son consideradas áreas seguras. Por ningún motivo debe ingresar personal no autorizado. Los medios donde se almacenan los backups no deben ser manipulados por personal sin la debida autorización.

- **Antes de realizar cambios sobre algún sistema de información, debe realizarse un backup.**

Explicación: Es necesario realizar un backup de cualquier sistema de información antes de cualquier cambio. Esto debe estar incluido en el proceso de gestión de cambios de la organización.

- **Antes de realizarse cualquier renovación tecnológica sobre las plataformas de backup, debe migrarse la información al nuevo sistema.**

Explicación: En caso de renovación tecnológica sobre plataformas que realizan backups y/o almacenamiento o sobre los sistemas de información en sí, debe asegurarse que la información que se encuentra en el sistema obsoleto, sea trasferida al nuevo sistema. Esto con el fin de evitar pérdidas de información en las transiciones tecnológicas.

3.4.5 Política de Uso de Estaciones de Trabajo

Estas políticas van dirigidas a todo el personal, contratistas y visitantes de SUPER INTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA Se espera que permitan definir los comportamientos esperados, para reducir la manifestación de riesgos que afecten la seguridad de la información de la empresa.
Los Gerentes y Coordinadores de cada área son responsables de velar por el cumplimiento de estas políticas. En caso de no entendimiento de las mismas, tramitar consulta al área de seguridad de la información de la empresa.

3.4.6 DIRECTRICES

- **Uso de estaciones de trabajo.**

Explicación: Las estaciones de trabajo entregadas a los colaboradores deberán estar plenamente identificadas, para ser usadas única y exclusivamente para el desarrollo de las actividades propias de su cargo; se prohíbe el almacenamiento de información personal en los equipos. El colaborador es el propietario responsable por la protección y cuidado de su equipo. En caso de finalización del vínculo laboral del colaborador esta deberá ser devuelta a la empresa.

- **Uso de dispositivos de almacenamiento externo**.

Explicación: El uso de dispositivos de almacenamiento externo estará restringido mediante la aplicación de políticas en los equipos, y únicamente para los colaboradores que lo requieran para desempeñar sus labores, se entregarán permisos para su uso por un periodo máximo de seis meses, que serán otorgados por el Jefe inmediato del colaborador respectivo, con el visto bueno del área de seguridad de la información. Una vez finalice su uso, su contenido será borrado a bajo nivel para evitar fugas de información.

- **Salida de equipos de las instalaciones.**

Explicación: La posibilidad de extraer estaciones de trabajo (desktops, laptops) fuera de las instalaciones por parte de los colaboradores, deberá estar autorizada por escrito por el jefe inmediato y con justificación de la necesidad. Estos permisos se entregarán semestralmente. En la salida y posterior reingreso de los equipos se deberá hacer un registro por parte del personal de seguridad. El colaborador deberá tomar precauciones para evitar el robo y daño de estos equipos fuera de las instalaciones.

- **Acceso a las estaciones de trabajo**.

Explicación: El acceso a estaciones de trabajo deberá realizarse mediante el usuario y contraseña propia de cada colaborador. El préstamo de usuarios y contraseñas está estrictamente prohibido bajo cualquier circunstancia. Se debe hacer buen uso de estas contraseñas, evitando su divulgación. Periódicamente

- **El uso de la solución corporativa de protección contra el Malware, es de carácter obligatorio para toda estación de trabajo asignada a cualquier colaborador de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA.**

- **Explicación:** Toda estación de trabajo de la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA,** deberá ejecutar una versión actualizada del software corporativo de protección contra el malware. Este software deberá ser capaz de proteger al sistema operativo en tiempo real y de actualizarse de forma automática.

- **Ningún usuario deberá desinstalar, desactivar y/o manipular ninguna pieza de software que no haya sido instalada por soporte técnico; esto podría ocasionar un riesgo alto de seguridad.**

Explicación: Se debe proteger la configuración instalada del software en cada estación de trabajo. Por lo tanto se prohíbe realizar cambios en estaciones de trabajo que permitan instalar nuevas piezas de software que no hayan sido autorizadas por la Coordinación de Soporte y Mantenimiento. También se exige la no manipulación por parte del usuario, de la configuración de la solución de protección contra el malware, para mantener para el nivel óptimo de seguridad a cada estación de trabajo.

- **Ningún usuario deberá manipular las piezas internas de hardware que compongan una estación de trabajo.**

Explicación: Se debe proteger la configuración instalada del hardware en cada estación de trabajo. Por lo tanto se prohíbe realizar cambios en estaciones de trabajo que modifiquen su integridad a nivel de hardware.

- **Por ningún motivo está permitida la creación y/o difusión de software malicioso.**

- **Explicación:** Bajo ninguna circunstancia los usuarios podrán escribir, compilar, copiar, propagar o ejecutar de forma intencionada en dispositivos tecnológicos de **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA.**, códigos o programas diseñados para replicarse, dañar o entorpecer el desempeño de cualquier sistema de información.

- **Buen uso del servicio de navegación a internet.**

Explicación: La finalidad de entregar el servicio de navegación en internet a los colaboradores y visitantes desde estaciones de trabajo, es para apoyar la realización de labores definidas en sus responsabilidades de cargo. Por lo anterior, se promueve el autocontrol por parte del colaborador para hacer buen uso de este servicio. En caso que se identifique mal uso del mismo, el colaborador será monitoreado, restringido y en caso que haya lugar sancionado.

- **Buen uso del servicio de correo electrónico.**

Explicación: La finalidad de entregar el servicio de correo electrónico es habilitar la comunicación interna y externa de colaboradores de la empresa. Se restringe su uso para propósitos personales, repartir cadenas de correos, o generar actividades no autorizadas por la empresa. Se utilizaran mecanismos para monitorear el buen uso del correo electrónico. En caso que el colaborador tenga cuentas de correo electrónico personales, estas no podrán: 1) Ser accedidas desde la red de la empresa, y 2) Ser utilizadas para propósitos laborales.

- **Atención de requerimientos relacionados con el uso de estaciones de trabajo.**

  Explicación: En caso de presentarse inestabilidad, degradación o fallas en las estaciones de trabajo, se deberá contactar al soporte técnico de la empresa a través de la mesa de servicio.

3.4.7 Política de seguridad Física y del Entorno

La seguridad física y del entorno juega un rol fundamental en la protección de la información y de los sistemas involucrados en el procesamiento de la misma. Debido a esto es importante definir unos lineamientos para garantizar que todos los colaboradores de LA SUPERINTENDENCIA DE INDISTRIA Y COMERCIO DE BOGOTA velen por la integridad y buen uso de los controles implementados.

En búsqueda de la alineación a las iniciativas desarrolladas por la organización en este campo de la seguridad, a continuación se menciona la política general que referencia las directrices definidas en el presente documento:
LA SUPERINTENDENCIA DE INDISTRIA Y COMERCIO DE BOGOTA., y sus directivas establecen dentro de las políticas, el compromiso para diseñar estrategias y mantener los niveles más altos posibles de Seguridad Física, propendiendo por la mitigación del riesgo que pueda atentar contra sus trabajadores y/o su planta física e infraestructura.

El personal directivo de LA SUPERINTENDENCIA DE INDISTRIA Y COMERCIO DE BOGOTA., será el responsable de asegurar el más alto nivel posible de Seguridad Física al interior de la compañía, teniendo en cuenta el cumplimiento a la normatividad vigente de la Superintendencia de Vigilancia y Seguridad Privada de la República de Colombia. Será obligación contractual de todos los

colaboradores y contratistas el estricto cumplimiento a la normatividad, Política de Seguridad Física y Consignas Particulares diseñadas para la protección del Recurso Humano, Planta Física e Infraestructura de la entidad.

3.4.8 DIRECTRICES.

- **Diseño y mantenimiento plan de seguridad física.**

Explicación: La empresa debe diseñar y gestionar un plan de seguridad física que sea revisado y actualizado anualmente. Este plan debe considerar la implementación y administración de los controles de seguridad física que busquen proteger las personas, los activos de información y los sistemas informáticos de las instalaciones físicas de la empresa, de amenazas de índole natural, generadas por el hombre o circunstanciales.

- **Control de acceso utilizando carnets de identificación.**

Explicación: El acceso de colaboradores a las instalaciones debe ser controlado mediante la exigencia del uso a toda hora de un carnet visible. El personal de seguridad debe monitorear la presencia de individuos sin carnet y solicitar la presentación del mismo. La lista de colaboradores debe ser revisada mensualmente y ajustada acorde al ingreso y salida de personal. Si un colaborador olvida su carnet, puede usar un carnet temporal después de haberse identificado. Se debe tener una bitácora de ingresos.

- **Identificar y limitar el acceso a áreas restringidas.**

Explicación: Las áreas restringidas deben estar plenamente identificadas en el plan de seguridad física de las instalaciones de la empresa. Los

colaboradores no autorizados no deben entrar a áreas restringidas. Se deben implementar controles de acceso independientes para estas áreas. No se debe utilizar los privilegios de acceso con el fin de permitir que entre una persona no autorizada.

- **Eliminación de carnet de identificación y contraseñas de acceso en la desvinculación del personal.**

Explicación: Cuando un colaborador finalice su contrato de trabajo, todos los códigos de acceso físico conocidos por esta persona deben ser desactivados. El carnet de identificación debe ser entregado a la entidad para ser destruido.

- **Controles de acceso a los visitantes/proveedores: identificación, registro y acompañamiento.**

Explicación: La llegada de un visitante o proveedor debe ser anticipada por los empleados de la empresa. El visitante debe llenar la bitácora de registro y reportar el ingreso de equipos de cómputo, los cuales deberán ser registrados por parte del personal de seguridad. La identificación de esta persona debe ser con un documento con foto. Los visitantes deben ser acompañados siempre por un colaborador de la entidad.

- **Registro de acceso a áreas seguras.**

Explicación: El trabajo en áreas seguras debe realizarse por personal autorizado. Por lo tanto se debe mantener una bitácora para registrar cada vez que un colaborador o visitante ingresa o sale a áreas seguras. Este registro debe detallar la fecha y hora de ingreso y debe mantenerse un mínimo de 3 meses.

- **Inspección de maletines.**

  Explicación: Los guardias de seguridad deben chequear los maletines de los colaboradores y visitantes, tanto al ingreso como a la salida de la empresa para identificar posibles situaciones de fuga de activos de información.

- **Control de ingreso y salida de dispositivos de almacenamiento extraíbles.**

  Explicación: Todo dispositivo de almacenamiento extraíble (memorias USB, discos duros externos, entre otros) deberá ser registrado al ingresar a las instalaciones de la empresa. Su autorización de uso será temporal y deberá ser aprobada por la gerencia respectiva de área, con el visto bueno del Área de Seguridad de la Información. Esto con la finalidad de verificar su justificación de uso y posibles riesgos asociados.

- **Pautas de seguridad en oficinas: escritorios limpios y bajo llave.**

  Explicación: Las oficinas de los empleados deben permanecer bajo llave cuando no se usen. No se deben dejar ningún elemento sobre los escritorios referente a información de trabajo. Los portátiles deben permanecer con guayas de seguridad y utilizar candados de llave o clave.

- **Pautas de seguridad en áreas seguras: uso equipos de cómputo y monitoreo.**

  Explicación: Las estaciones de trabajo y equipos de computación en áreas seguras deben estar ubicados y protegidos adecuadamente, según la naturaleza de la confidencialidad del proceso y de la información que se maneja. Estos equipos deben tener implementados procedimientos de seguridad que certifiquen su adecuado uso, y evitar así fugas de

información. Los colaboradores deben estar monitoreados mediante CCTV de forma permanente.

- **Administración de equipos de CCTV.**

Explicación: Las grabaciones de video con uso de CCTV deben ser monitoreadas y almacenadas con los mecanismos de seguridad y disponibilidad adecuados para su revisión. Las cintas deben almacenar grabaciones por un periodo mínimo de 2 meses.

- **Seguridad en la recepción de correspondencia y/o envíos.**

Explicación: Los documentos y/o envíos recibidos se deben almacenar en un área restringida (solo ingresa personal autorizado) y deben estar debidamente identificados y señalizados, con el fin de evitar fuga de información y perdida de activos.

La llegada de un transportador debe ser anticipada para disponer el personal y el espacio requerido. El personal de seguridad física y de inventario debe registrar la novedad de ingreso o salida de elementos en la bitácora, realizando las inspecciones necesarias.

3.4.9 Política de protección contra el Malware.

Cada día los sistemas de información son más propensos a la amenaza creciente llamada Malware. Por tanto es relevante definir las directrices mínimas de control, que permitan mantener protegidos los sistemas de almacenamiento y/o procesamiento de información en la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA.

3.4.10 DEFINCION

Malware: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

3.4.11 DIRECTRICES.

La Empresa dispondrá de la solución corporativa de protección contra el Malware que considere apropiada para la protección de sus activos de información, teniendo en cuenta lo síguete:

- **Se debe diseñar, documentar, socializar e implementar procedimientos de protección contra el Malware.**

  Explicación: Los usuarios serán garantes de la primera línea de protección de los sistemas de información con los cuales interactúan. Por tanto es necesario suministrar instructivos que les oriente acerca de las acciones a tomar, cuando se evidencia malware en los sistemas de información. Estos instructivos deben definir claramente las fases de prevención, contención y erradicación del malware.

- **El administrador de la solución de protección contra el Malware deberá diseñar y aplicar manuales y procedimientos de operación.**

  Explicación: Se debe desarrollar y/o identificar documentación actualizada y práctica en relación con la administración de la solución de protección contra el Malware. Esta documentación debe contemplar aspectos tales como: guías de instalación, configuración, administración, atención de

problemas y escalamiento con terceros. El administrador debe demostrar competencia en su uso y entendimiento.

- **Las estaciones de trabajo de la empresa deben estar equipadas de la solución corporativa de protección contra el Malware.**

Explicación: Al momento de alistar una estación de trabajo se debe instalar, configurar y actualizar la solución corporativa de protección contra el malware.

- **Los servidores de la empresa deben contemplar los mecanismos de protección contra el Malware.**

Explicación: Al momento de alistar un servidor se debe considerar la instalación, configuración y actualización de la solución corporativa de protección contra el malware. En caso de no instalación de esta solución, se deben desarrollar las actividades de aseguramiento necesarias para la protección contra el malware.

- **La solución corporativa de protección contra el malware debe ser capaz de proteger al S.O. en tiempo real y de actualizarse de forma automática.**

Explicación: Los sistema de información de la empresa, deben estar bajo el alcance de la solución corporativa de protección contra el malware; por ningún motivo los usuarios modificaran los parámetros de configuración de esta solución. Solo se podrá realizar bajo autorización del área encargada de la administración del servicio.

- **Todos los usuarios de los sistemas de información de LA SUPER INTENDENCIA FINANCIERA DE INDUSTRIA Y COMERCIO DE BOGOTA., serán garantes del óptimo funcionamiento del sistema de protección contra el malware**

  Explicación: Cuando se evidencie cualquier anomalía referente al tema aquí descrito, deberá ser reportado de manera inmediata al área de seguridad de la información por medio de los canales establecidos; quienes se encargaran de la atención oportuna del evento.

3.4.12 Política de Gestión de Incidentes en la Seguridad de la Información.

La gestión de respuesta a incidentes en Seguridad de la Información para la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA es un componente primordial en los programas de IT (Information Technology), el cual es el servicio base del CSIRT (Computer Security Incident Response Team) y en español (Equipo de Respuesta ante Emergencias Informáticas organizacional) para su funcionamiento.

3.4.13 DIRECTRICES.

- **Compromiso de la alta dirección en la gestión de incidentes en seguridad de la información.**

  Explicación: La alta dirección de la empresa reconoce y respalda la importancia de gestionar los incidentes en seguridad de la información y declara su compromiso en el cumplimiento de los objetos contractuales, la normatividad y legislación aplicable para la atención de estos incidentes.

- **Detección de eventos en seguridad de la información.**

  Explicación: Los sistemas informáticos de la empresa deben tener la capacidad de registrar y permitir la recolección de información pertinente para determinar las causas de un posible incidente en seguridad de la información con la finalidad de conservar la trazabilidad de un evento ocurrido.

- **Comunicación de incidentes y/o anomalías en seguridad de la información.**

  Explicación: Los eventos relativos que conduzcan a una incidencia en seguridad de la información serán comunicados a través de la Mesa de Servicio de la empresa, describiendo la situación presentada y se trataran con la mayor confidencialidad. Está establecerá los mecanismos de escalamiento necesarios para su atención y respuesta.

- **Priorización de incidentes en seguridad de la información.**

  Explicación: Basados en la valoración de impacto y urgencia en seguridad de la información, se dará priorización a los incidentes presentados con la finalidad de brindar la atención y respuesta apropiada.

- **Contactos y asesoramiento de atención y respuesta a incidentes en seguridad de la información.**

  Explicación: Identificadas las capacidades necesarias que requieran la atención y respuesta a incidentes en seguridad de la información, se establecerán contactos y acuerdos con organizaciones especializadas para

su tratamiento, con la finalidad de brindar capacidades de respuesta competentes y diligentes según la magnitud del incidente.

- **Recolección de evidencia legal aplicable ante incidentes en seguridad de la información.**

  Explicación: Con la finalidad de identificar responsable(s) y un resarcimiento del daño ocasionado para aplicar una acción jurídica, se propenderá recolectar, mantener y presentar evidencia cumpliendo con la normatividad legal aplicable.

3.4.14 Política de Seguridad para la Gestión de la Red de Datos.

Para la adecuada administración de la red de datos de la SUPER INTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA, es necesaria la declaración de reglas a nivel de seguridad, que permitan establecer consideraciones mínimas aceptables para garantizar la disponibilidad, confidencialidad e integridad de la información que es transportada por la misma.
La infraestructura de red de datos y la seguridad de la información son componentes que deben ir acompañados de la mano, a fin de dar cumplimiento a la política.

Esta política aplica para toda la infraestructura de networking administrada por el proceso de soporte de servicios organizacional, donde se busca la defínción, implementación, monitoreo, soporte y mantenimiento de una arquitectura de red de datos que brinde niveles aceptables de seguridad, la cual garantice los controles y niveles autoritativos de conectividad.

3.4.15 DIRECTRICES

- **Para la adecuada protección de los sistemas de información conectados a la red de datos de La Empresa, se debe desarrollar y mantener de una arquitectura perimetral por capas donde se establezcan normas de configuración para la inspección y control del tráfico.**

  Explicación: Con la finalidad de gestionar la seguridad de la red de datos administrada, se debe implementar y mantener una arquitectura perimetral que permita por medio de la segmentación física y lógica, la definición de zonas (Internet, DMZ, Granja de Servidores) y capas de seguridad a través de cortafuegos (firewalls), el control del tráfico entrante y saliente necesario del entorno de datos de los sistemas de información.

- **Se debe deshabilitar todos aquellos servicios, parámetros y puertos de red que no sean necesarios para el funcionamiento de la infraestructura de red, garantizando los criterios mínimos de seguridad.**

  Explicación: Para mitigar los riesgos de seguridad asociados a los dispositivos de red de La Empresa, se deben deshabilitar aquellos servicios, parámetros y puertos de red que por defecto traen activos y que no se requieren para el funcionamiento del servicio, al igual que las interfaces que no estén operativas. Se deben garantizar los criterios mínimos de configuración segura establecidos en modelo de seguridad de la organización.

- **La configuración de enrutadores, switchs, firewalls, sistemas de detección y prevención de intrusos de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la administración de la red de datos.**

  Explicación: Los administradores de la red de datos deben mantener un adecuado registro documental que permita tener trazabilidad de la gestión de la red de datos de La Empresa. De igual forma conforme a los cambios desarrollados se debe generar y administrar backups de la configuración activa para la restauración en caso de fallas.

- **Todo dispositivo de networking deberá ser revisado, registrado y aprobado por la administración del área de plataforma antes de conectarse a la red de datos de La Empresa.**

  Explicación: Para el correcto registro y permisos de conectividad necesarios de los dispositivos que necesiten conectarse a la red de datos de La Empresa, se debe notificar la necesidad al Área de Plataforma para su autorización. Dicha área, debe desconectar aquellos dispositivos que no están aprobados y reportar tal conexión como un incidente en seguridad de la información a ser investigado.

- **El acceso a la red de datos de La Empresa y conectividad a los sistemas de información soportados por la misma es de carácter restringido. Se concederán permisos en base a "la necesidad de conocer" y los criterios de seguridad de la información contemplados en la presente política.**

Explicación: Los permisos de acceso a la red de datos y los recursos respaldados por la solución perimetral de La Empresa, se concederán en base a los criterios definidos en la arquitectura de seguridad definida y la "necesidad de conocer".

Dichos permisos serán administrados por las áreas de plataforma y seguridad de la información, la cuales desarrollarán una revisión periódica de cada seis (6) meses a fin de garantizar las necesidades organizacionales y la integridad del modelo de seguridad de la información.

- **La transmisión de datos corporativa a través de redes públicas, se debe desarrollar por medio de mecanismos de cifrado a fin de garantizar la confidencialidad e integridad de la información.**

Explicación: La información confidencial y sobre la cual debe garantizarse su integridad, (basados en su criticidad y sensibilidad) se debe cifrar por medio de mecanismos seguros (Ej. SSL/TLS, IPSEC) durante su transmisión a través de las redes donde el acceso es abierto y/o sin restricción.

- **La supervisión y monitoreo de la red de datos de La Empresa, debe ser respaldada a través de mecanismos de registro de actividades, para prevención, detección o minimización de impacto de riesgos asociados a la seguridad de la información.**

Explicación: Se deben implementar mecanismos de registro y monitoreo para la supervisión del tráfico transportado por las redes de datos administradas por La Empresa. Esto permitirá el rastreo, análisis y

generación de reportes ante eventos adversos que atenten contra la seguridad de la información de la organización.

- **Las conexiones de acceso remoto deberán ser estrictamente controladas bajo el esquema avalado por el área de Seguridad de la Información y gestionado por la administración del área de plataforma de La Empresa.**

  Explicación: Para la adecuada gestión de las conexiones remotas (Ej. VPN, RDP) estas deberán ser suministradas a través de las soluciones adquiridas formalmente por La Empresa para su estricto control. Se prohíbe la utilización de clientes de conexión remota que no están avalados por el área de Seguridad de la Información para este tipo de actividad y cuya gestión este por fuera de los ámbitos de administración del área de gestión de plataforma de La Empresa.

  Las conexiones remotas que se efectúen por fuera de la red corporativa, es responsabilidad del funcionario y/o colaborador al cual se le ha otorgado permisos de acceso, el garantizar el nivel mínimo aceptable de seguridad de la información para la adecuada utilización del recurso.

- **El uso de analizadores de red (sniffers), es permitido única y exclusivamente para el Área de Seguridad de la Información y los administradores de la red de datos de La Empresa.**

  Explicación: Para monitorear la funcionalidad de las redes que están bajo la gestión administrativa de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA, el uso de software que permite analizar tráfico de red (sniffers), debe ser utilizado única y exclusivamente por el personal

de seguridad de la información y los administradores de redes que la organización designe para dicha roll, enfocados a la consolidación del modelo de seguridad de La Empresa y la resolución de incidencias.

3.4.16 Política de Identificación y Control de Activos de la Empresa.

El control de activos de información constituye uno de los puntos más importantes a tener en cuenta en la construcción de un modelo de seguridad. Debido a la criticidad que estos tienen dentro de la operación y a la sensibilidad de los datos que manejan, cualquier robo, perdida o fuga puede representar un riesgo de alto impacto para la empresa.

3.4.17 DIRECTRICES.

- **Definición de lineamientos para la identificación de activos de información.**

  Explicación: El área de seguridad de la información debe definir y comunicar los lineamientos para la identificación y control de los activos de información de la empresa. Estableciendo así el nivel de profundidad y alcance en la identificación de los activos de información. Especificando los que se consideren de principal atención por parte de la gestión en seguridad de la información.

- **Realización de inventario de activos información, asignación de propietarios y custodios**.

  Explicación: Cada Jefe de Área con el acompañamiento del área de seguridad de la información anualmente deberá tipificar, inventariar y clasificar los activos de información que son utilizados por la empresa. El área de seguridad comunicará las responsabilidades de los propietarios y

custodios de estos activos de información. Este inventario será notificado al área de seguridad de la información, que se encargará de validar el cumplimiento de estas responsabilidades. En caso de modificaciones o traslados de estos activos de información, estas deberán ser notificadas al área de seguridad de la información para la actualización del registro correspondiente.

- **Clasificación y Etiquetamiento de Activos de Información.**

  Explicación: Cada activo de información deberá ser clasificado y etiquetado según su valor, criticidad y sensibilidad. Este nivel de clasificación se establecerá conforme a unos parámetros generales de disponibilidad y confidencialidad del activo de información.

- **Entrega de activos de información**

  Explicación: La entrega de activos de información a los colaboradores deberá realizarse únicamente bajo autorización del jefe inmediato y previa evaluación de la necesidad. Se deberá realizar un acta para registrar la entrega y la responsabilidad de custodia y protección por parte del colaborador.

4. CONCLUSIONES

- En la investigación realizada en la SIC se concluye que al no tener un marco de políticas definidas y aunque el área de tecnología tiene algunos controles internos es fundamental que se sigan lineamientos para la seguridad de la información y no estar expuestos a ataques de robo de información.

- De acuerdo al diagnóstico realizado la seguridad de la información se identifica como áreas vulnerables

  - área de centro de documentación e información
  - Centro de cómputo por acceso de no autorizado.

- Dadas las políticas de seguridad informática en la entidad permiten el mejoramiento continuo de los diferentes elementos que lo componen por tanto es indispensable concienciar al personal de dichas políticas para contribuir al cumplimento de las mismas.

5. RECOMENDACIONES

Como recomendaciones adicionales a las ya planteadas anteriormente se sugiere lo siguiente:

- La entidad considere a largo plazo hacer un plan de migración de datos a una base de datos más robusta, ya que la utilizada actualmente puede servir como de respaldo en el sector para así obtener beneficios en su producción.

- Se podría considerar tener un departamento de desarrollo y conocimiento donde la empresa pueda explotar aún más las ideas de sus empleados y puedan llegar a ser líderes en calidad de sus productos.

- En el área de gestión humana, a largo plazo al tener implementadas las recomendaciones que se dieron anteriormente se pueden hacer planes de retención del mejor personal para tener competitividad de cargos profesionales y empezar a atraer al personal más capacitado, ya que al contar con un personal idóneo, la entidad se vuelve más competitiva e innovadora en cuanto a procesos, productos y seguridad.

REFERENCIAS BIBLIOGRAFICAS

❖ Textos y Publicaciones.

- Aguilera, P. (2010). *SEGURIDAD INFORMATICA* . Madrid España: EDITEX S.A.
- Bertolin, J. A. (2008). *Seguridad de la Informacion ,Redes Informatica y sistemas de informacion.* Madrid(España): Paraninfo.
- Cerra, M. (2010). *200:Respuestas_Seguridad.* Lomas de Zamora : Fox Andina Gradi S.A.
- Diaz, G., Mur, F., San Cristobal, E., Castro, A.-M., & Peire, J. (2012). *Seguridad en las Comunicaciones y en la Infiormacion.* Madrid(España): Uned.
- Heredero, C. D., Lopez, J. J., Agius, H., Romero Romero, S. M., Medina Salgado, S., Navarro Montero, A., & Sanchez Najera, J. J. (2006). *Direccion y Gestion de los Sistemas de Informacion en la empresa.* Pozuelo de Alarcon (Madrin): ESIC seguna edicion.
- Royer, J.-M. (2004). *Seguridad en la Informatica de empresa.* Cornella de Llobregat(Barcelona): Eni.
- Estrada, A. C. (2011). *Seguridad por Niveles.* Madrid(España): Darfe.
- Yost, J. R. (2007). A history of computer security standards. *Elsiever*, 595-621.

❖ INFOGRAFIA

- Academic, 2. (2015). *http://advisera.com/27001academy/es/que-es-iso-27001/*. Obtenido de http://advisera.com/27001academy/es/que-es-iso-27001/
- Colombia.com. (1999). Obtenido de http://www.colombia.com/tecnologia/derechos-de-autor-propiedad-intelectual/nacional/ley-lleras.aspx: http://www.colombia.com/tecnologia/derechos-de-autor-propiedad-intelectual/nacional/ley-lleras.aspx
- Docsetools. (2015). *docsetools*. Obtenido de http://docsetools.com/articulos-enciclopedicos/article_80922.html#
- E. Vicente, ,. A.-M. (2014). *Elsevier*, 1-12.
- HERNÁNDEZ, R. (2000). eguridad en las redes e Internet. *Boletín de Política Informática N° 2*, 7. Obtenido de https://www.segu-info.com.ar/firewall/firewall.htm
- Kenneth J. Knappa, ,. ,. (2009). Information security policy: An organizational-level process model. *Elsevier*, 493–508.
- Mariua erbana, *. R.-M. (2014). Information Protection – Security, Clustering and E-governance. *Procedia*, 288-292.
- MINITIC. (s.f.). *MINITIC*. Obtenido de MINITIC: www.mintic.gov.co/portal/604/articles-3705_documento.pdf
- *Segu.Info*. (2009). Obtenido de https://www.segu-info.com.ar/proteccion/vulnerar.htm
- *Segu.Info*. (2009). Obtenido de https://www.segu-info.com.ar/malware/spyware.htm
- SIC. (2015). *http://www.sic.gov.co/drupal/mision-y-vision*.
- UNAD. (25 de MARZO de 2015). *UNAD*. Recuperado el 03 de MAYO de 2015, de UNAD: http://gidt.unad.edu.co/leyesinformaticas
- *Universidad Autonoma de Mexico*. (2014). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ISO27.php
- *Universidad Autonoma de Mexico*. (2014). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServiciosSeguridad.php

RELACION DE ANEXOS

Anexo A: Lista de diagnóstico de vulnerabilidades de la SIC.

Fuente: Soporte estructurado con base en la norma ISO/IEC 27001:2006

Anexo B: Matriz de Riesgo.

Anexo C: Norma ISO/IEC 27001:2006.

ANEXO A: LISTA DE DIAGNÓSTICO DE VULNERABILIDADES DE LA SIC.

A.5 POLITICA DE SEGURIDAD				
A.5.1 Política de la seguridad de la información. Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y leyes pertinentes.			**CUMPLE**	**NO CUMPLE**
A.5.1.1	Documento de la política de seguridad de la información	La dirección de la SIC cuenta con un documento de políticas de seguridad de la información y lo publica y comunica a todos los empleados y partes externas pertinentes.		X
A.5.1.2	Revisión de la política de seguridad de la información.	La política de seguridad de la información se revisa a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.		X

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION				
A.6.1 Organizacfion Interna. Objetivo: Gestionar la seguridad de la informacion dentro de la organización				
			CUMPLE	NO CUMPLE
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Se tiene definido e implementado un proceso de autorización de la dirección de la SIC para nuevos servicios de procesamiento de información.	X	
A.6.1.5	Acuerdos sobre confidencialidad	Se identifican y revisan con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	X	
A.6.1.6	Contacto con las autoridades	Se mantenienen contactos apropiados con las autoridades pertinentes.	X	
A.6.1.7	Contacto con grupos de interés especiales	Se mantenienen los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	X	
A.6.1.8	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se revisan independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.		X

A.6.2 PARTES EXTERNAS. Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas				
			CUMPLE	NO CUMPLE
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Se identifican los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.	X	
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Todos los requisitos de seguridad identificados se consideran antes de dar acceso a los clientes a los activos o la información de la organización	X	
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información se consideran todos los requisitos pertinentes de seguridad		X

A.7 GESTION DE ACTIVOS				
A.7.1 Responsabilidad por los activos. Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.				
			CUMPLE	NO CUMPLE
A.7.1.1	Inventario de activos.	Todos los activos estan claramente identificados y se tiene elaborado y actualizado un inventario de todos los activos importantes de la SIC.	X	
A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con los servicios de procesamiento de información deben estan designados a una parte designada de la organización.	X	
A.7.1.3	Uso aceptable de los activos	Se identifican, documentan e implementan las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	X	

A.7.2 CLASIFICACION DE LA INFORMACION Objetivo: asegurar que la información recibe el nivel de protección adecuado.				
			CUMPLE	NO CUMPLE
A.7.2.1	Directrices de clasificación.	La información se encuentra clasificada en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	X	
A.7.2.2	Etiquetado y manejo de información	Se desarrollan e implementan un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	X	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS				
Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.				
			CUMPLE	NO CUMPLE
A.8.1.1	Roles y responsabilidades	Se deben definen y documentan los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	X	
A.8.1.2	Selección	Se realizan revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener	X	
A.8.1.3	Términos y condiciones laborales.	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes estan de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	X	

A.8.2 Durante la vigencia de la contratación laboral

Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

			CUMPLE	NO CUMPLE
A.8.2.1	Responsabilidades de la dirección	La dirección de la SIC exige que los empleados,contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	x	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes reciben formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	x	
A.8.2.3	Proceso disciplinario	Existe un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	X	

A.7 GESTION DE ACTIVOS

A.7.1 Responsabilidad por los activos. Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.

			CUMPLE	NO CUMPLE
A.7.1.1	Inventario de activos.	Todos los activos estan claramente identificados y se tiene elaborado y actualizado un inventario de todos los activos importantes de la SIC.	X	
A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con los servicios de procesamiento de información deben estan designados a una parte designada de la organización.	X	
A.7.1.3	Uso aceptable de los activos	Se identifican, documentan e implementan las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	X	

A.7.2 CLASIFICACION DE LA INFORMACION Objetivo: asegurar que la información recibe el nivel de protección adecuado.				
			CUMPLE	NO CUMPLE
A.7.2.1	Directrices de clasificación.	La información se encuentra clasificada en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	X	
A.7.2.2	Etiquetado y manejo de información	Se desarrollan e implementan un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	X	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS				
Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.				
			CUMPLE	NO CUMPLE
A.8.1.1	Roles y responsabilidades	Se deben definen y documentan los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	X	
A.8.1.2	Selección	Se realizan revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener	X	
A.8.1.3	Términos y condiciones laborales.	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes estan de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	X	

A.8.2 Durante la vigencia de la contratación laboral

Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

			CUMPLE	NO CUMPLE
A.8.2.1	Responsabilidades de la dirección	La dirección de la SIC exige que los empleados,contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	x	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes reciben formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	x	
A.8.2.3	Proceso disciplinario	Existe un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	X	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

A.8.3 Terminación o cambio del contratación laboral

Objetivo: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada..

			CUMPLE	NO CUMPLE
A.8.3.1	Responsabilidades en la terminación	Se definen y asignan claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	X	
A.8.3.2	Devolución de activos	Todos los empleados, contratistas o usuarios de terceras partes devuelven todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	X	
A.8.3.3	Retiro de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se retiran al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	X	

A.9 SEGURIDAD FÍSICA Y DEL ENTORNO				
A.9.1 Áreas seguras Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.				
			CUMPLE	NO CUMPLE
A.9.1.1	Perímetro de seguridad física	Se utilizan perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	X	
A.9.1.2	Controles de acceso físico.	Las áreas seguras estan protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X	
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Se tiene diseñado y aplicado la seguridad física para oficinas, recintos e instalaciones		X
A.9.1.4	Protección contra amenazas externas y ambientales.	Se diseñan y aplican protecciones físicas contra daño por incendio, inundación,terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	X	
A.9.1.5	Trabajo en áreas seguras.	Se diseñan y aplican la protección física y las directrices para trabajar en áreas seguras.	X	
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se estan controlados y, si es posible, aislados de los servicios de procesamiento de información para evitar el acceso no autorizado.	X	

A.9 SEGURIDAD FÍSICA Y DEL ENTORNO				
A.9.2 Seguridad de los equipos Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.				
			CUMPLE	NO CUMPLE
A.9.2.1	Ubicación y protección de los equipos.	Los equipos estan ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.		X
A.9.2.2	Servicios de suministro	Los equipos estan protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.		X
A.9.2.3	Seguridad del cableado.	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información estan protegidos contra interceptaciones o daños.	X	
A.9.2.4	Mantenimiento de los equipos.	Los equipos reciben mantenimiento adecuado para asegurar su continua disponibilidad e integridad.		X
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	Se suministra seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.		X
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos.	Se verifican todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles y aseguran que se hayan sobrescrito de forma segura, antes de la eliminación.	X	
A.9.2.7	Retiro de activos	Los equipo, información y software se retiran con autorización previa.	X	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES				
A.10.1 Procedimientos operacionales y responsabilidades Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.			**CUMPLE**	**NO CUMPLE**
A.10.1.1	Documentación de los procedimientos de operación	Los procedimientos de operación se encuentran documentados, y estan disponibles para todos los usuarios que los necesiten.	X	
A.10.1.2	Gestión del cambio.	Se controla los cambios en los servicios y los sistemas de procesamiento de información.	X	
A.10.1.3	Distribución de funciones.	Las funciones y las áreas de responsabilidad se distribuyen para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	X	
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Las instalaciones de desarrollo, ensayo y operación estan separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.		X

A.10.2 Gestión de la prestación del servicio por terceras partes Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.				
			CUMPLE	NO CUMPLE
A.10.2.1	Prestación del servicio	Se garantiza que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, son implementados, mantenidos y operados por las terceras partes.	X	
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Los servicios, reportes y registros suministrados por terceras partes se controlan y revisan con regularidad y las auditorias se llevan a cabo a intervalos regulares.	X	
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se gestionan teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	X	

A.10.3 Planificación y aceptación del sistema

Objetivo: minimizar el riesgo de fallas de los sistemas.

			CUMPLE	NO CUMPLE
A.10.3.1	Gestión de la capacidad.	Se hace seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	X	
A.10.3.2	Aceptación del sistema.	Se establecen criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevan a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	X	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

A.10.4 Protección contra códigos maliciosos y móviles

Objetivo: proteger la integridad del software y de la información.

			CUMPLE	NO CUMPLE
A.10.4.1	Controles contra códigos maliciosos.	Se implementan controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.		X
A.10.4.2	Controles contra códigos móviles	Cuando se autoriza la utilización de códigos móviles, la configuración se asegura que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se evita la ejecución de los códigos móviles no autorizados.	X	

A.10.5 Respaldo

Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de linformación.

			CUMPLE	NO CUMPLE
A.10.5.1	Respaldo de la información.	Se hacen copias de respaldo de la información y del software, y se ponen a prueba con regularidad de acuerdo con la política de respaldo acordada.	X	

A.10.6 Gestión de la seguridad de las redes

Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

			CUMPLE	NO CUMPLE
A.10.6.1	Controles de las redes.	Las redes mantienen y controlan adecuadamente para protegerlas de las amenazas y se mantiene la seguridad de los sistemas y aplicaciones que usan la red, incluyendo lainformación en tránsito.	X	
A.10.6.2	Seguridad de los servicios de la red.	En cualquier acuerdo sobre los servicios de la red se identifican e incluyen las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.	X	

A.10.7 Manejo de los medios

Objetivo: evitar la divulgación , modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

			CUMPLE	NO CUMPLE
A.10.7.1	Gestión de los medios removibles	Se establecen procedimientos para la gestión de los medios removibles	X	
A.10.7.2	Eliminación de los medios.	Cuando ya no se requieran estos medios, su eliminación se hace de forma segura y sin riesgo, utilizando los procedimientos formales.	X	
A.10.7.3	Procedimientos para el manejo de la información.	Se establecen procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	X	
A.10.7.4	Seguridad de la documentación del sistema.	La documentación del sistema esta protegida contra el acceso no autorizado.	X	

A.10.8 Intercambio de la información Objetivo: mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.				
			CUMPLE	NO CUMPLE
A.10.8.1	Políticas y procedimientos para el intercambio de información	Se establecen políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	X	
A.10.8.2	Acuerdos para el intercambio	Se establecen acuerdos para el intercambio de la información y del software entre la organización y partes externas.	X	
A.10.8.3	Medios físicos en tránsito.	Los medios que contienen información se protegen contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	X	
A.10.8.4	Mensajería electrónica.	La información contenida en la mensajería electrónica tiene la protección adecuada		X
A.10.8.5	Sistemas de información del negocio.	Se establecen, desarrollan e implementan políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.	X	

A.10.9 Servicios de comercio electrónico Objetivo: garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.				
			CUMPLE	NO CUMPLE
A.10.9.1	Comercio electrónico	La información involucrada en el comercio electrónico que se transmite por las redes públicas esta protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	X	
A.10.9.2	Transacciones en línea	La información involucrada en las transacciones en línea esta protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración , divulgación , duplicación o repetición no autorizada del mensaje.	X	
A.10.9.3	Información disponible al público	La integridad de la información que se pone a disposición en un sistema de acceso público esta protegida para evitar la modificación no autorizada.	X	

A.10.10 Monitoreo Objetivo: detectar actividades de procesamiento de la información no autorizadas.				
			CUMPLE	NO CUMPLE
A.10.10.1	Registro de auditorías	Se elaboran y mantienen durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	X	
A.10.10.2	Monitoreo del uso del sistema	Se establecen procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se revisan con regularidad.	X	
A.10.10.3	Protección de la información del registro	Los servicios y la información de la actividad de registro se protegen contra el acceso o la manipulación no autorizados.	X	
A.10.10.4	Registros del administrador y del operador	Se registran las actividades tanto del operador como del administrador del sistema..	X	
A.10.10.1	Registro de fallas	Las fallas se registran y analizan, y se toman las acciones adecuadas.	X	
A.10.10.1	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad estan sincronizados con una fuente de tiempo exacta y acordada.	X	

A.11 CONTROL DE ACCESO **A.11.1 Requisito del negocio para el control de acceso** Objetivo: controlar el acceso a la información.				
			CUMPLE	NO CUMPLE
A.11.1.1	Política de control de acceso	Se establecen, documentan y revisan la políticas de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	X	

A.11.2 Gestión del acceso de usuarios

Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

			CUMPLE	NO CUMPLE
A.11.2.1	Registro de usuarios.	Existe un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	X	
A.11.2.2	Gestión de privilegios	Se restringe y controla la asignación y uso de privilegios.	X	
A.11.2.3	Gestión de contraseñas para usuarios.	La asignación de contraseñas controla a través de un proceso formal de gestión.	X	
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	La dirección de la SIC establece un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	X	

A.11.3 Responsabilidades de los usuarios

Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

			CUMPLE	NO CUMPLE
A.11.3.1	Uso de contraseñas.	Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	X	
A.11.3.2	Equipo de usuario desatendido.	Los usuarios se aseguran de que a los equipos desatendidos se les da protección apropiada.		X
A.11.3.3	Política de escritorio despejado y de pantalla despejada	Se adopta una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	X	

A.11.4 Control de acceso a las redes

Objetivo: evitar el acceso no autorizado a servicios en red.

			CUMPLE	NO CUMPLE
A.11.4.1	Política de uso de los servicios de red.	Los usuarios sólo tienen acceso a los servicios para cuyo uso están específicamente autorizados.		X
A.11.4.2	Autenticación de usuarios para conexiones externas.	Se emplean métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	X	
A.11.4.3	Identificación de los equipos en las redes.	La identificación automática de los equipos cuenta con un medio para autenticar conexiones de equipos y ubicaciones específicas.	X	
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	El acceso lógico y físico a los puertos de configuración y de diagnóstico estan controlados.	X	
A.11.4.5	Separación en las redes.	En las redes se separan los grupos de servicios de información, usuarios y sistemas de información.	X	
A.11.4.6	Control de conexión a las redes.	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se restringen la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio.	X	
A.11.4.7	Control de enrutamiento en la red.	Se implementan controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	X	

A.11.5 Control de acceso al sistema operativo

Objetivo: evitar el acceso no autorizado a los sistemas operativos.

			CUMPLE	NO CUMPLE
A.11.5.1	Procedimientos de ingreso seguros	El acceso a los sistemas operativos se controla mediante un procedimiento de registro de inicio seguro.	X	
A.11.5.2	Identificación y autenticación de usuarios.	Todos los usuarios cuentan con un identificador único (ID del usuario) únicamente para su uso personal, y se tiene una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	X	
A.11.5.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas son interactivos y aseguran la calidad de las contraseñas.	X	
A.11.5.4	Uso de las utilidades del sistema	Se restringe y controlan estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	X	
A.11.5.5	Tiempo de inactividad de la sesión	Las sesiones inactivas se suspenden después de un periodo definido de inactividad.	X	
A.11.5.6	Limitación del tiempo de conexión.	Se utilizan restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	X	

A.11.6 Control de acceso a las aplicaciones y a la información

Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.

			CUMPLE	NO CUMPLE
A.11.6.1	Restricción de acceso a la información.	Se restringe el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	X	
A.11.6.2	Aislamiento de sistemas sensibles.	Los sistemas sensibles tienen un entorno informático dedicado (aislados).	X	

A.11.7 Computación móvil y trabajo remoto

Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

			CUMPLE	NO CUMPLE
A.11.7.1	Computación y comunicaciones móviles.	Se establece una política formal y se adoptan las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	X	
A.11.7.1	Trabajo remoto.	Se desarrollan e implementan políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	X	

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

A.12.1 Requisitos de seguridad de los sistemas de información

Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.

			CUMPLE	NO CUMPLE
A.12.2.1	Análisis y especificación de los requisitos de seguridad	Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes especifican los requisitos para los controles de seguridad.	X	

A.12.2 Procesamiento correcto en las aplicaciones

Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

			CUMPLE	NO CUMPLE
A.12.2.1	Validación de los datos de entrada.	Se validan los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	X	
A.12.2.2	Control de procesamiento interno.	Se incorporan verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	X	
A.12.2.3	Integridad del mensaje.	Se identifican los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	X	
A.12.2.4	Validación de los datos de salida.	Se validan los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.	X	

A.12.3 Controles criptográficos

Objetivo: proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.

			CUMPLE	NO CUMPLE
A.12.3.1	Política sobre el uso de controles criptográficos.	Se desarrolla e implementa la política sobre el uso de controles criptográficos para la protección de la información.		X
A.12.3.2	Gestión de llaves.	Se tiene implementado un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.		X

A.12.4 Seguridad de los archivos del sistema

Objetivo: garantizar la seguridad de los archivos del sistema.

			CUMPLE	NO CUMPLE
A.12.4.1	Control del software operativo.	Se implementan procedimientos para controlar la instalación de software en sistemas operativos.	X	
A.12.4.2	Protección de los datos de prueba del sistema.	Los datos de prueba se seleccionan cuidadosamente, se encuentran protegidos y se tiene un control de estos.	X	
A.12.4.3	Control de acceso al código fuente de los programas	Se restringe el acceso al código fuente de los programas.	X	

A.12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.

			CUMPLE	NO CUMPLE
A.12.5.1	Procedimientos de control de cambios.	Se controla la implementación de cambios utilizando procedimientos formales de control de cambios.	X	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se revisan y someten a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	X	
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Se desalienta la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se controlan estrictamente.	X	
A.12.5.4	Fuga de información	Se evitan las oportunidades para que se produzca fuga de información.		X
A.12.5.5	Desarrollo de software contratado externamente	La organización supervisa y monitorea el desarrollo de software contratado externamente.	X	

A.12.6 Gestión de la vulnerabilidad técnica

Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

			CUMPLE	NO CUMPLE
A.12.6.1	Control de vulnerabilidades técnicas	Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluan la exposición de la organización a dichas vulnerabilidades y se toman las acciones apropiadas para tratar los riesgos asociados.	X	

A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

			CUMPLE	NO CUMPLE
A.13.1.1	Reporte sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se informan a través de los canales de gestión apropiados tan pronto como sea posible.	X	
A.13.1.2	Reporte sobre las debilidades de la seguridad	Se exige a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	X	

A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

			CUMPLE	NO CUMPLE
A.13.2.1	Responsabilidades y procedimientos	Se establecen las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X	
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Existen mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	X	
A.13.2.3	Recolección de evidencia	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se recolecta,retiene y se presenta para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	X	

A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio

Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

			CUMPLE	NO CUMPLE
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Se desarrollan y mantiene un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	X	
A.14.1.2	continuidad del negocio y evaluación de riesgos	Se identifican los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	X	
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Se desarrollan e implementan planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.	X	
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Se mantiene una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	X	
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Los planes de continuidad del negocio se someten a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	X	

A.15 CUMPLIMIENTO

A.15.1 Cumplimiento de los requisitos legales

Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

			CUMPLE	NO CUMPLE
A.15.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se definen explícitamente, se documentan y se mantener actualizados para cada sistema de información y para la organización	X	
A.15.1.2	Derechos de propiedad intelectual (DPI).	Se implementan procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	X	
A.15.1.3	Protección de los registros de la organización.	Los registros importantes se encuentran protegidos contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	X	
A.15.1.4	Protección de los datos y privacidad de la información personal.	Se garantiza la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	X	
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Se disuaden a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	X	
A.15.1.6	Reglamentación de los controles criptográficos.	Se utilizan controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	X	

A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico

Objetivo: asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización..

			CUMPLE	NO CUMPLE
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	Los directores garantizan que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.	X	
A.15.2.2	Verificación del cumplimiento técnico.	Los sistemas de información verifican periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	X	

A.15 CUMPLIMIENTO A.15.3 Consideraciones de la auditoría de los sistemas de información Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.				
			CUMPLE	NO CUMPLE
A.15.3.1	Controles de auditoría de los sistemas de información.	Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se planifican y se acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	X	
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Se protege el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.	X	

ANEXO B: MATRIZ DE RIESGO

PROBABILIDAD	VALOR	IMPACTO	VALOR
ALTA	3	ALTO	3
MEDIA	2	MEDIO	2
BAJA	1	BAJO	1

NIVEL DE RIESGO	VALOR
BAJO TOLERABLE	1,2 Y 3
MEDIO-NO ACEPTABLE	4 Y 6
ALTO CRITICO	9

N°	RIESGO	PROBABILIDAD	VALOR	IMPACTO	VALOR	NIVEL DE RIESGO	VALOR	PLAN DE MITIGACIÓN DEL RIESGO
1	Los mecanismos de revisión de la seguridad informática en todas las áreas de la SIC son inadecuadas.	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Diseñar un marco de políticas enfocadas en la protección de los datos y fugas de información.
2	Fugas de información con terceras partes	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	validar que todos los puertos se encuentren deshabilitados para terceras partes y fomentar el uso de correos electrónicos corporativos
3	Daño físico o perdida datos (Instalaciones viejas)	BAJA	1	ALTO	3	ACEPTABLE	3	Realizar backups de la información para evitar la perdida ante daño físico de los equipos. Firmar pólizas de aseguramiento de los equipos para mitigar la perdida económica.
4	Las instalaciones para el centro de computo no tienen medidas de seguridad física.	BAJA	1	BAJO	1	ACEPTABLE	1	Realizar el análisis de riesgos físicos para determinar los controles necesarios para evitar accesos no deseados.
5	No es evidente un plan de mantenimiento de equipos activos	ALTA	3	ALTO	3	ALTO CRÍTICO	9	Realizar mantenimiento periódicos de los equipos de la SIC.
6	El control de accesos y salidas de equipos no están establecidas	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Se debe controlar los ingresos y las salidas de equipos con bitácoras de seguridad.
7	No se establecen correctamente los enlaces de separación de instalaciones del área de desarrollo con las áreas de operación	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Antes de realizar el traslado del centro de computo principal, verificar las conexiones de usuarios
8	Falla en la protección de los datos por mensajería electrónica	ALTA	3	ALTO	3	ALTO CRÍTICO	9	se debe encriptar los mensajes de correos electrónicos para evitar el uso inadecuado de la información
9	Falla en el mantenimiento de equipos desatendidos	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Generar una ventana de mantenimiento para el traslado de equipos desatendidos
10	Fugas de información por puertos usb externos de equipos activos	ALTA	3	ALTO	3	MEDIO-NO ACEPTABL	6	validar que todos los puertos se encuentren deshabilitados
11	caída o interrupción del servicio	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Generar una ventana de mantenimiento para el traslado, contando con la funcionalidad de contingencia en caso de ser necesario. Realizar dicha ventana en un horario de bajo uso.
13	Suspensión indefinida del centro de computo principal.	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Para mitigar este riesgo se propone poner en servicio los servidores de contingencia para que ellos presten el servicio.
14	Falla en el centro de computo de contingencia.	BAJA	1	ALTO	3	ACEPTABLE	3	Realizar pruebas del centro de computo de contingencia estableciendo métricas óptimas de medición de los tiempos de subida de los servicios y realizar los ajustes si es necesario, de acuerdo a la información suministrada en las mediciones.
15	La Red eléctrica del centro de computo es inadeacuada	ALTA	3	ALTO	3	ALTO CRÍTICO	9	Establecer el nivel de consumo de los dispositivos del centro de computo para establecer la potencia eléctrica requerida antes de realizar el
16	Perdida de información durante la suspensión de la replica.	BAJA	1	MEDIO	2	ACEPTABLE	2	Antes de para la replica garantizar que ningún usuario este conectado.
17	Las instalaciones para el centro de computo no tienen medidas de seguridad física.	BAJA	1	BAJO	1	ACEPTABLE	1	Realizar el análisis de riesgos físicos para determinar los controles necesarios para evitar accesos no deseados.
18	Las medidas del rack en el centro de computo son inadecuadas.	ALTA	3	MEDIO	2	MEDIO-NO ACEPTABL	6	Usar las misma marca y especificaciones de los racks del centro de computo principal. Tener una lista de chequeo con el fin de de verificar las medidas de estructurales. Tener los números de contacto de proveedores para gestionar inmediatamente cualquier cambio o solicitar apoyo ante cualquier inconveniente.
19	Un sistema de información sin bloqueo por el usuario.	MEDIA	2	ALTO	3	MEDIO-NO ACEPTABL	6	Colocar incidentes de seguridad a los usuarios que no tengan un manejo adecuado de los equipos de la entidad

ANEXO C: